REMARKS

Applicants have studied the Final Office Action dated June 4, 2007 and have made amendments to claims 1, 9, 10, 15, and 20-22. No new matter was added. Reconsideration and allowance of the pending claims in view the following remarks are respectfully requested. Applicants submit that the application is in condition for allowance. In the Office Action, the Examiner:

- Objected to claim 1 because of various informalities;
- Rejected claims 20-22 under 35 U.S.C. § 101 for being directed towards software per se; and
- Rejected claims 1-22 under 35 U.S.C. § 103(a) as being unpatentable over Circenis (U.S. Patent Publication 2004/0054908 in view of The IBM Certification Study Guide AIX V4.5 System Administration (1999).

Claim Objections

As noted above, the Examiner objected to claim 1 because of various informalities. The Applicants have amended claim 1 to recite "diagnose" as compared to "diagnosis" as suggested by the Examiner. Therefore, the Applicants respectfully suggest that the objection to claim 1 has been overcome and should be withdrawn.

Rejection under 35 U.S.C. § 101

As noted above, the Examiner rejected claims 20-22 under 35 U.S.C. § 101. With respect to claims 20-22, the Applicants have amended claims 20-22 to more clearly recite "A computer readable storage medium analyzing software running in a tamper-resistant environment, the computer readable storage medium comprising instructions for:" Support for this amendment where the product is shipped and executed on a client computer is described on page 16, lines 3-6 of the application as originally filed.

No new matter has been added. Applicants respectfully assert that independent claim 20, and the dependencies thereunder, are now statutory subject matter. Applicant respectfully requests that the rejection be withdrawn.

Rejections under 35 U.S.C. § 103(a)

As noted above, the Examiner rejected claims 1-22 under 35 U.S.C. § 103(a) as being unpatentable over Circenis (U.S. Patent Publication 2004/0054908) in view of The IBM Certification Study Guide AIX V4.5 System Administration (1999). Independent claims 1, 10, 15, and 20 have been amended to more clearly recite the present invention.

In particular, independent amended claim 1 now more clearly recites:

> A system that allows analysis of software running in a tamper-resistant environment, the system comprising:
>
> a processor which monitors at least one instance of software execution identified and selected by a user to be monitored and creates a log entry with at least one set of data derived from the one instance of software execution, whereby the set of data is used to diagnose the software execution;
>
> an encryption system which generates at least one symmetric key and encrypts the log entry for the at least one set of data using the symmetric key, wherein the encryption system encrypts the symmetric key using a public key associated with the encryption system;
>
> a log file of a relatively-fixed size which stores the log entry for the at least one set of data which has been encrypted, and wherein the log file includes the symmetric key which has been encrypted with the public key;
>
> random data in the log file when it is originally created and which is replaced by log entries so that a size of the log file including log entries appears to be a substantially constant size; and
>
> a pointer which identifies a next storage location for a next log entry so that a last log entry can be determined and the next log entry can be positioned in a location in the log file after a previous log entry.

Support for this claim is found at page 9, lines 1-7, page 15, line 9 through page 16, line 15 and FIG. 3 elements 86 and 88. No new matter has been added. The present invention uses management where:

> an encryption system which generates at least one symmetric key and encrypts the log entry for the at least one set of data using the symmetric key, wherein the encryption system encrypts the symmetric key using a public key associated with the encryption system;
>
> a log file of a relatively-fixed size which stores the log entry for the at least one set of data which has been encrypted, and wherein the log file includes the symmetric key which has been encrypted with the public key;

This prevents the public key (if found in the tamper-resistant program file) from being substituted with a known public-key from an attacker's keypair.

Independent claims 10, 15, and 20 have also been amended similar to claim 1 above. The arguments and remarks presented below also apply to independent claims 10, 15, and 20 as well.

With respect to claim 1, the Examiner states on page 4 of the Final Office Action that Circenis teaches "a processor which monitors at least one instance of software execution identified and selected by a user to be monitored and creates a log entry with at least one of a set of data is used to diagnose the software execution". The Examiner supports this assertion by stating Circenis teaches "'[u]sing the tamper-evident system 200 of FIG. 3, a sender is able to monitor and control application utilization by collecting data associated with the application, creating tamper-evident data records, and providing the tamper-evident data records" (Circenis at paragraph [0037).

The Applicants would like to clearly point out that a "user" in the presently claimed invention is completely different from a "sender" as taught by Circenis. As expressly taught by Circenis, the sender is the data owner (See Circenis, for example, at

paragraph [0018]), whereas a user in the presently claimed invention is an end user or an IT professional. In other words, Circenis is directed at monitoring content usage and tampering of content control policies (See Circenis generally), while the present invention is directed at debugging an application running within a protected environment (See the Specification as originally filed at, for example, pages 3, 7, and 14).

The customer of Circenis is more comparable to the user of the presently claimed invention, where the customer of Circenis is actually using the application, music file, etc. Nowhere does Circenis teach or suggest "a processor which monitors at least one instance of software execution identified and selected by a user to be monitored" (emphasis added). In fact, Circenis teaches away from this claim element. The entire purpose of Circenis is to detect any tampering of a file by a user. Therefore, if a user was given the ability to turn on/off logging as recited for the presently claimed invention, the tamper-evident management system in Circenis would be defeated.

The argument made with respect to the Naslund reference in the previous Response With Amendment dated March 21, 2007 is also applicable to Circenis. For example, the monitoring of the presently claimed invention can only be for <u>one instance of software execution</u> and does not have to be for every instance. Circenis, on the other hand, is completely silent on this claim element. For example, Circenis teaches a metering application that collects "metrics data associated with operation of the computer system" whenever a user uses an application. See Circenis at paragraph [0019]. If a user uses an application 5 times, Circenis teaches that usage information for each of the 5 times is recorded. Assuming arguendo that Circenis and the presently claimed invention teaches logging and monitoring the same type of data (which they do not), Circenis would have to teach that of the 5 times an application is used a user can select which of the 5 times data should be logged. Circenis clearly does not teach this. In fact, this is completely against what Circenis is trying to accomplish as stated above.

Therefore, Circenis does not teach "a processor which monitors at least one instance of

software execution identified and selected by a user to be monitored and creates a log entry with at least one set of data derived from the one instance of software execution, whereby the set of data is used to diagnose the software execution". Accordingly, claim 1 (and claims 10, 15, and 20), distinguishes over Circenis for at least these reasons.

Furthermore, dependent claim 7 (and similarly claims 11, and 16) further recites "wherein the system further includes a mechanism for receiving an input from a user that initiates logging of log entries into the log file each time logging is desired by the user". The Examiner states that Circenis teaches "[t]he iCOD computer could save usage data to a log file or a central metering device that a vendor employee could check periodically by visiting the site". The Examiner further states that the Examiner "*interprets the vendor employee as the user the (sic) indicates logging is desired*".

The Applicants respectfully suggest that the Examiner has mischaracterized Circenis. A vendor employee does not go to the "site" to initiate logging. The citation of paragraph [0024] clearly states that the vendor employee goes to the "site" to check the usage data that has been saved. The Examiner is improperly characterizing Circenis to read on the present claim element. Accordingly, claims 7, 11, 16, distinguish over Circenis for at least these reasons.

The Examiner further states that Circenis teaches "an encryption system which encrypts the log entry for the at least one set of data (Figure 4 teaches encrypting the log entry for at least one set of data, particularly step 320 'Sign data entry with application private key', step 325 'Encrypt with vendor public key' and step 330 'Store in data log'"). However, claim 1 (and similarly claims 10, 15, and 20) now more clearly recites "an encryption system which generates at least one symmetric key and encrypts the log entry for the at least one set of data using the symmetric key, wherein the encryption system encrypts the symmetric key using a public key associated with the encryption system using a public key associated with the encryption system". Nowhere does Circenis teach a symmetric key, let alone a symmetric key used to encrypt log

entry. Furthermore, nowhere does Circenis teach that a public key is used to encrypt the symmetric key. This is advantageous because a user or other party is unable to discern which piece of data within the log file is the symmetric key.

Furthermore, claim 1 (and similarly claims 10, 15, and 20) also recites "a log file of a relatively-fixed size which stores the log entry for the at least one set of data which has been encrypted, and wherein the log file includes the symmetric key". Nowhere does Circenis teach that the log file includes the symmetric key. Circenis is completely silent on this claim element. Accordingly, claim 1 (and claims 10, 15, and 20), distinguishes over Circenis for at least these reasons.

The Examiner correctly states on pages 4-5 of the Final Office Action that Circenis "does not explicitly teach a log file of a relatively-fixed size which stores the log entry for the at least one set of data which have been encrypted". However, the Examiner combines Circenis with the IBM reference to overcome the deficiencies of Circenis. In particular, the Examiner states that the IBM reference teaches "*[t]he alog (sic) command can maintain and manager logs. It reads standard inpu (sic), writes to standard output, and copies the output into a fixed-sized file. This file is treated as a circular log"*.

The Examiner also correctly states that Circenis and the IBM reference do not explicitly teach "random data in the log file when it is originally created and which is replaced by log entries so that a size of the log including log entries appears to by a substantially-constant size"). The Examiner goes on to state "It would have been obvious to one or ordinary skill in the art at the time of the invention to insert random data into the log file when it is initially created. The motivation is that it is inherent that the circular log is of a fixed size so it must be initialized with some values. One of ordinary skill in the art would know how to initialize the circular log with random values."

The Applicants respectfully disagree. The Examiner is incorrect in stating that it is

obvious to insert random data in a log file and that a fixed size file must be initialized with some values. First, it is not customary to always insert random data into log files. Second, fixed-size files do not have to be initialized with random data. A fixed-sized file such as that taught by the IBM reference can be defined as a file that cannot exceed a certain size. For example, if the file is fixed at 100 bytes, the file can comprise any number of bytes from 0 to 100, but not exceed 100 bytes. The presently claimed invention, on the other hand, inserts random data into the log file at its creation so that the log file appears to be a substantially constant size no matter how many log entries are in the log file.

For example, the Specification as originally filed at patents 18-19 states "By using the system shown in FIG. 7, the log file remains of a size for n entries, which means that the log file remains substantially the same size at all times. In this case, the physical log file appears to be the size of n entries, even when it has no real entries (upon creation in FIG. 7a) or when it has two entries (in FIG. 7b) or when n+1 entries have been created and the file includes the last n entries (in FIG. 7c). However, this would differ from a normal log file that starts at a small size before the logging starts and grows as the logging continues. Such a log file keeps growing larger as the logging continues, giving evidence of a new logged transaction (data being logged) by looking at the file before and after, whereas the system of the present invention does not show a change in size whether a transaction has occurred and logging has happened or not."

Therefore, the inherency argued by the Examiner does not exist. If the presently claimed element is inherent and obvious, then the Applicants respectfully request that the Examiner provide references teaching "…a log file of a relatively-fixed size which stores the log entry for the at least one set of data which has been encrypted, and wherein the log file includes the symmetric key which has been encrypted with the public key; random data in the log file when it is originally created and which is replaced by log entries so that a size of the log file including log entries appears to be a

substantially constant size…" Accordingly, claim 1 (and similarly claims 10, 15, and 20) distinguishes over Circenis alone and/or in view of the IBM reference.

For the foregoing reasons, Claims 1-22 distinguish over Circenis alone and/or in combination with the IBM reference. Claims 2-9, 11-14, 16-19, and 21-22 depend from claims 1, 10, 15, and 20, respectively. Since dependent claims include all the limitations of the independent claims, claims 2-9, 11-14, 16-19, and 21-22 distinguish over Circenis alone and/or in combination with the IBM reference, as well. Accordingly, Applicants believe that the rejection under 35 U.S.C. § 103(a) has been overcome and respectfully request that this rejection be withdrawn.

CONCLUSION

Applicants acknowledge the continuing duty of candor and good faith to disclosure of information known to be material to the examination of this application. In accordance with 37 CFR § 1.56, all such information is dutifully made of record. The foreseeable equivalents of any territory surrendered by amendment is limited to the territory taught by the information of record. No other territory afforded by the doctrine of equivalents is knowingly surrendered and everything else is unforeseeable at the time of this amendment by the Applicants and their attorneys.

Applicants respectfully submit that all of the grounds for rejection stated in the Examiner's Office Action have been overcome and that all claims in the application are allowable. No Previously Presented matter has been added. It is believed that the application is now in condition for allowance or alternatively is in better form for consideration on appeal, which allowance is respectfully requested.

The Commissioner is hereby authorized to charge any fees that may be required or credit any overpayment to Deposit Account 09-0460. In view of the preceding

discussion, it is submitted that the claims are in condition for allowance. Reconsideration and re-examination is requested.

PLEASE CALL the undersigned if that would expedite the prosecution of this application.

Respectfully Submitted,

Date: September 4, 2007

/Jon A. Gibbons/
Attorney for the Applicants
Jon A. Gibbons
(Reg. No. 37,333)

Fleit, Kain, Gibbons, Gutman,
Bongini & Bianco P.L.
551 N.W. 77th Street, Suite 111
Boca Raton, FL 33487
Telephone No.: (561) 989-9811
Facsimile No.: (561) 989-9812